AMENDMENTS TO THE CLAIMS

1.-7. (Canceled)

8. (Currently amended) A method for use in generating digital signatures in an information processing system, the system including at least a user device, an intermediary device and a verifier, the method comprising the steps of:

generating in the user device a first digital signature; and

sending the first digital signature to the verifier;

wherein the verifier sends the first digital signature to the intermediary device, and the intermediary device checks that the first digital signature is a valid digital signature for the user device and if the first digital signature is valid generates a second digital signature which is returned to the verifier as a signature generated by the user device;

wherein the second digital signature is generated using a second secret key associated with second digital signature protocol having a computational efficiency lower than that of the first digital signature protocol;

wherein the second digital signature is generated using a second secret key associated with second digital signature protocol having a computational efficiency lower than that of the first digital signature protocol;

~~The method of claim 3~~ wherein the verifier upon receipt of the first digital signature checks that the first digital signature is a valid digital signature using a first public key corresponding to the first secret key.

9.-10. (Canceled)

11. (Currently amended) A method for use in generating digital signatures in an information processing system, the system including at least a user device, an intermediary device and a verifier, the method comprising the steps of:

generating in the user device a first digital signature; and

sending the first digital signature to the verifier;

wherein the verifier sends the first digital signature to the intermediary device, and the intermediary device checks that the first digital signature is a valid digital signature for the user device and if the first digital signature is valid generates a second digital signature which is returned to the verifier as a signature generated by the user device;

wherein the first digital signature is generated using a first secret key associated with a first digital signature protocol having a computational efficiency compatible with computational resources of the user device;

~~The method of claim 2~~ wherein the verifier upon receipt of the second digital signature checks that the second digital signature is a valid digital signature using a second public key corresponding to the second secret key.

12. (Currently amended) A method for use in generating digital signatures in an information processing system, the system including at least a user device, an intermediary device and a verifier, the method comprising the steps of:

generating in the user device a first digital signature; and

sending the first digital signature to the verifier;

wherein the verifier sends the first digital signature to the intermediary device, and the intermediary device checks that the first digital signature is a valid digital signature for the user device and if the first digital signature is valid generates a second digital signature which is returned to the verifier as a signature generated by the user device;

~~The method of claim 1~~ wherein the user device is switchable between a normal operating mode and a secure operating mode.

13. (Currently amended) A method for use in generating digital signatures in an information processing system, the system including at least a user device, an intermediary device and a verifier, the method comprising the steps of:

generating in the user device a first digital signature; and

sending the first digital signature to the verifier;

wherein the verifier sends the first digital signature to the intermediary device, and the intermediary device checks that the first digital signature is a valid digital signature for the user device and if the first digital signature is valid generates a second digital signature which is returned to the verifier as a signature generated by the user device;

~~The method of claim 1~~ wherein the first digital signature is generated only after user verification of the message to be signed.

14. (Currently amended) A method for use in generating digital signatures in an information processing system, the system including at least a user device, an intermediary device and a verifier, the method comprising the steps of:

generating in the user device a first digital signature; and

sending the first digital signature to the verifier;

wherein the verifier sends the first digital signature to the intermediary device, and the intermediary device checks that the first digital signature is a valid digital signature for the user device and if the first digital signature is valid generates a second digital signature which is returned to the verifier as a signature generated by the user device;

~~The method of claim 1~~ wherein at least one of first and second secret keys used to generate the respective first and second and second digital signatures are stored in an at least partially encrypted form on the user device and the intermediary device, respectively.

15. (Currently amended) A method for use in generating digital signatures in an information processing system, the system including at least a user device, an intermediary device and a verifier, the method comprising the steps of:

generating in the user device a first digital signature; and

sending the first digital signature to the verifier;

wherein the verifier sends the first digital signature to the intermediary device, and the intermediary device checks that the first digital signature is a valid digital signature for the user

device and if the first digital signature is valid generates a second digital signature which is returned to the verifier as a signature generated by the user device;

~~The method of claim 1~~ wherein at least one of first and second secret keys used to generate the respective first and second and second digital signatures is configured such that a first portion thereof is stored in the user device and a second portion thereof is stored in a storage element removable from the user device.

16. (Currently amended) A method for use in generating digital signatures in an information processing system, the system including at least a user device, an intermediary device and a verifier, the method comprising the steps of:

generating in the user device a first digital signature; and

sending the first digital signature to the verifier;

wherein the verifier sends the first digital signature to the intermediary device, and the intermediary device checks that the first digital signature is a valid digital signature for the user device and if the first digital signature is valid generates a second digital signature which is returned to the verifier as a signature generated by the user device;

~~The method of claim 1~~ wherein if a user associated with the user device can contact the intermediary device and upon providing an access code thereto direct the intermediary device not to generate the second digital signature.

17. (Canceled)

18. (Currently amended) A method for use in generating digital signatures in an information processing system, the system including at least a user device, an intermediary device and a verifier, the method comprising the steps of:

generating in the user device a first digital signature; and

sending the first digital signature to the verifier;

wherein the verifier sends the first digital signature to the intermediary device, and the

intermediary device checks that the first digital signature is a valid digital signature for the user device and if the first digital signature is valid generates a second digital signature which is returned to the verifier as a signature generated by the user device;

~~The method of claim 1~~ wherein the user device precomputes a plurality of coupons, a given one of the coupons being utilizable to generate the first digital signature.

19-25. (Canceled)